5A-2

ソフトウェア設計に適用する複数ガイドライン間の用語揺れとその対策

小林　大樹†　　塚本　良太†　　山田　亮†　　田村　孝之†

三菱電機株式会社　情報技術総合研究所†

1. はじめに

安全なソフトウェアの作成のために、ソフトウェアの脆弱性の網羅的な抽出と、脆弱性への対策の適用が急務となっている。脆弱性のチェック手法としては情報セキュリティの専門家によるレビューが一般的であるが、この方法は専門家を長期間拘束することとなり、コスト増を招きやすい。

本研究では、ソフトウェアの脆弱性への対策を効率化するため、情報セキュリティの専門家がソフトウェアの脆弱性とその対策について整理した複数のガイドライン（例えば[1][2]等）をベースとして、非専門家（一般のソフトウェア開発者等）が開発対象ソフトウェアの脆弱性をチェックする手法について検討する。

2. 複数ガイドラインに基づく脆弱性チェック方式とその課題

本研究ではソフトウェアの脆弱性や対策について非専門家に一元的かつ網羅的に提示できる方式について検討する。そのため、本研究ではガイドラインを集約してデータベース化し、集約されたガイドラインの項目（以下、ガイド項目という）を、ガイドラインの用語（以下、ガイド用語という）でキーワード検索するというアプローチを採用した。本研究の脆弱性チェック方式のモデルを図 1に示す。

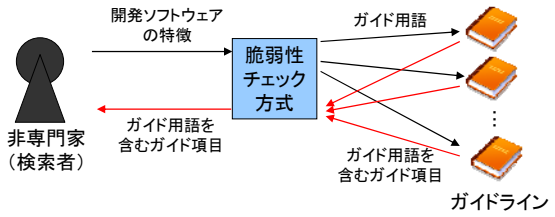


図 1 脆弱性チェック方式のモデル

本方式は非専門家によって入力された開発対象のソフトウェアの特徴を解析することで、関連するガイド項目を複数のガイドラインから網羅的に検索する。なお、ソフトウェアの特徴の入力方法については[3]を参照されたい。ここで、本方式にはガイドラインの特性に基づく下記 3 点の課題がある。

課題 1.

ガイドライン間で用語が標準化されていないため、同じ表記のガイド用語が異なる意味を示す、あるいは異なる表記のガイド用語が同じ意味を示す「用語揺れ」が存在する。そのため、用語揺れがあるガイド用語でガイドラインの項目を検索しても、検索されるガイド項目は意図した検索結果と比較して過不足が生じ得る。例えば[1]において MAC は Message Authentication Code を意味するが、[2]では Media Access Control を意味するガイド用語として定義されているため、検索結果に冗長なガイド項目が混入し得る。

課題 2.

要素技術や攻撃手法の進歩に伴い、新たなガイドラインの追加や、既存ガイドラインの更新に伴うガイド項目やガイド用語の追加・変更が発生するため、それらに追随する必要がある。特に、追加・更新されたガイド用語は既存のガイド用語との用語揺れが発生し得るため、前記課題 1 と同様に、検索結果の過不足が新たに生じる。

課題 3.

他のガイド用語の総称等、意味の抽象度が異なるガイド用語があり、それらを他のガイド用語と同一視すると、本質的には無関係なガイド項目まで一緒に検索されてしまう。

3. 課題の解決策

課題を解決可能なガイド用語テーブルについて説明する。

3.1. ガイド用語テーブル

ガイド用語テーブルはガイド用語を管理するためのテーブルで、各ガイド用語はガイド用語の意味を示す一般的な概念を表す索引と、「同義」や「包含」等の関係性によって関連付けられることを対応関係として定義され、ガイド用語テーブルの項目として記録される。また、対応関係によって、そのガイド用語を使うガイドラインを示すガイドライン名とも関連付けられ

Handling Synonymous Terms in Different Guidelines for Software Design
Taiki KOBAYASHI, Ryota TSUKAMOTO, Ryo YAMADA and Takayuki TAMURA†.
†Information Technology R&D Center, Mitsubishi Electric Corporation.

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.

る。ガイド用語テーブルを図 2に示す。

索引	関係性	ガイド用語	ガイドライン名
認証	包含	MAC	ガイドライン_X
MACアドレス	同義	MAC	ガイドライン_Y
⋮	⋮	⋮	⋮

図 2 ガイド用語テーブル

図 2では、課題 1 で示した MAC というガイド用語が、異なるガイドラインで違う意味を示す語であることを定義できることを例示している。

以下、本方式が課題を解決できることを示す。

課題 1 の解決.

ガイドライン毎にガイド用語を分類することで、同じ表記のガイド用語が異なる意味を示す場合でも、各ガイドラインに応じてガイド用語を区別して選択できる。また、索引によってガイド用語を分類することで、異なる表記のガイド用語が同じ意味を示す場合でも、各ガイド用語の示す意味を索引から区別できるので、課題 1 を解決できる。

課題 2 の解決.

ガイド項目やガイド用語の追加・変更があった場合は、それらに関するガイド用語についてのみ、対応関係の追加・修正を行えばよい。この変更は他の対応関係には影響を与えないため、新たな用語揺れの発生について考慮する必要はない。また、検索されるガイド項目は定義された対応関係によってのみ定まるため、適切にガイド用語テーブルの対応関係を追加・変更することでガイド項目の追加や変更に対応できるので、課題 2 を解決できる。

課題 3 の解決.

対応関係の意味を関係性によって区別できるので、索引が示す意味と直接関連するガイド項目（同義）や、関連するが本質的なトピックは異なるガイド項目（包含）等を区別して検索することで課題 3 を解決できる。

3.2. 拡張された方式の動作

拡張されたガイドラインベース脆弱性チェック方式の動作を表 1に示す。

表 1 ソフトウェアの脆弱性チェック手法の動作

ステップ	動作
①	情報セキュリティの専門家が、ガイド用語テーブルに全てのガイド用語の対応関係を設定する。
②	非専門家がソフトウェアの特徴を入力し、[3]の方法により関連する索引を取得する。
③	ガイド用語テーブルを用い、索引と対応関係が定義されたガイド用語を取得する。
④	取得した全てのガイド用語で各ガイドラインのガイド項目を検索する。
⑤	関係性毎にガイド項目を分類して非専門家に提示する。

3.3. 考察

3.3.1. 本方式の実現性

本方式を実現するためには、索引とガイド用語の対応関係を定義する作業が重要となる。本方式の原理上、必要な対応関係の個数はガイド項目の総数の数倍程度と見積もれる。ここで事前の検討から、Web 関連ソフトウェアの設計・開発に関する著名な 13 ガイドラインに、脆弱性に関するガイド項目が 760 件あることが分かっており、これらの検索を目的とした場合、本方式は十分現実的な作業量で実現可能と期待できる。

3.3.2. 本方式の応用

本稿では情報セキュリティに注目して説明したが、本方式は用語揺れのある文献の検索全般に適用可能で、具体例としてソフトウェア開発における特定業種向けの法規制や商慣習に固有の知識等を説明したガイドライン等が挙げられる。本方式を応用することで、上記の専門知識を検索者に分かりやすく提示可能と考えられる。

4. まとめ

本稿ではソフトウェアの脆弱性チェックを効率化するため、集約された複数のガイドラインから、脆弱性のチェックに必要なガイドライン項目の一元的かつ網羅的な検索を実現する方式について述べた。本方式でガイド用語テーブルを管理することで、用語揺れやガイドラインの追加や更新に容易に対応可能であるという特長を持つ。今後、本方式を実装することでソフトウェア脆弱性のチェックを実際に行い、本方式の効果を定量的に確認する。

参考文献

[1] Security Standards Council, Payment Card Industry (PCI) データセキュリティ基準 要件とセキュリティ評価手順 バージョン 2.0, 2010.

[2] IPA, クラウドコンピューティング 情報セキュリティに関わる利点、リスクおよび推奨事項 (Cloud Computing Benefits, risks and recommendations for information security), 2009.

[3] 塚本良太, 小林大樹, 山田亮, 田村孝之, ソフトウェア設計におけるセキュリティ脆弱性の検索方式, 情報処理学会全国大会, 2014.

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.